[Insert Cover Picture]

Freight Rail Explosion Tabletop Exercise

Situation Manual

[Insert Date]

**\*[Insert Caveat]\***

This Situation Manual (SitMan) provides exercise participants with all necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 8:30 a.m. | 9:00 a.m. | Welcome and Introductions |
| 9:00 a.m. | 10:00 a.m. | Module One: Pre-Incident Information Sharing |
| 10:00 a.m. | 10:15 a.m. | Break |
| 10:15 a.m. | 11:15 a.m. | Module Two: Incident Response |
| 11:30 a.m. | 11:45 a.m. | Break |
| 11:45 a.m. | 12:45 p.m. | Module Three: Short-Term Recovery |
| 12:45 p.m. | 1:00 p.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Freight Rail Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX planned for [insert exercise duration] and will focus on [insert scope].This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP). |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response, and Recovery [Select appropriate Mission Area(s)]  |
| **Capabilities** | * Economic Recovery
* Intelligence and Information Sharing
* Mass Care Services
* On-Scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
* Planning
* Public Information and Warning
* Risk Management for Protection Programs and Activities
* Supply Chain Integrity and Security
* [Insert additional capabilities as necessary]
 |
| **Objectives** | 1. Examine pre-incident threat intelligence, information sharing, and notification and communication procedures between public and private sector partners including identifying threat assessment procedures, prevention resources and programs, and discussing pertinent privacy protection concerns.
2. Discuss coordination between private sector organizations and responding local, state, and federal agencies under the Incident Command System (ICS) / National Incident Management System (NIMS).
3. Examine public messaging and media relations procedures during and immediately following an incident.
4. Discuss recovery and continuity plans and procedures following an incident with a focus on business continuity and community recovery.
5. [Insert additional exercise objectives as necessary]
 |
| **Threat or Hazard** | Improvised Explosive Device (IED) with Hazardous Materials (HAZMAT) release |
| **Scenario** | An interactive, discussion-based exercise focused on a domestic threat and subsequent domestic incident at a freight yard. The scenario consists of three modules: Pre-Incident Information Sharing, Incident Response, and Short-Term Recovery. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Examine pre-incident threat intelligence, information sharing, and notification and communication procedures between public and private sector partners including identifying threat assessment procedures, prevention resources and programs, and discussing pertinent privacy protection concerns.  | * Intelligence and Information Sharing
* Operational Coordination
* Planning
* Risk Management for Protection Programs and Activities
 |
| Discuss coordination between private sector organizations and responding local, state, and federal agencies under ICS / NIMS. | * Mass Care Services
* On-Scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
* Planning
 |
| Examine public messaging and media relations procedures during and immediately following an incident. | * Operational Communications
* Public Information and Warning
 |
| Discuss recovery and continuity plans and procedures following an incident with a focus on business continuity and community recovery.  | * Economic Recovery
* Public Information and Warning
* Supply Chain Integrity and Security
 |
| [Insert additional objectives as necessary]. | * [Insert additional core capabilities as necessary].
 |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players** have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitators** provide situation updates and moderate the discussion. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Moderators** are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
* **Data Collectors** are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

## Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

* Module One: Pre-Incident Information Sharing
* Module Two: Incident Response
* Module Three: Short-Term Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of [insert mission areas] issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s / organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission areas] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

# Module One: Pre-Incident Information Sharing

## Scenario

### [Insert Month, Day, Year]: [Insert time]

Several weeks ago, federal agents prevented an attempted bombing at a bus station terminal in [insert city in nearby state]. The bomber indicated he’s a part of a larger plan. Based on this prevented attack and the bomber’s warnings of similar attacks, the Secretary of the Department of Homeland Security (DHS), in coordination with other federal entities, issued an “Elevated” Threat Alert through the National Terrorism Advisory System (NTAS), warning of a credible terrorist threat against the United States. There is no specific information at this time that would warrant the release of an “Imminent” Threat Alert **(See Appendix B)**.

The alert indicates all transportation system operators should be on high alert over the next four months, ending on [insert end date as indicated in Appendix B]. While there are no specific locations regarding where the next attack might take place, information from the captured bomber leads law enforcement to believe [insert your state] is a possible target.

## Discussion Questions

1. How does your organization receive NTAS alerts?
2. What information does your organization expect to receive from local, state, or federal entities?
	1. How long does it take for information to be processed for sharing?
	2. To whom and how is this information shared?
3. What role do local, state, and federal entities have in sharing information about a credible threat?
4. What federal resources might you employ at this time?
5. How does this NTAS alert change your security position?
6. How would your organization receive information about credible threat?
	1. Are there any government clearance considerations or issues?
7. How does your agency or organization triage intelligence information you receive, such as from formal reporting, hearsay, and social media?
8. Does your organization regularly communicate or meet with other regional transportation public sector stakeholders?
	1. Following the issuance of the NTAS alert, what communications might you expect from these relevant public sector transportation stakeholders?
	2. How might you share protection and prevention best practices with other freight yards?

## Scenario Update

## [Insert location]

### [Insert Month, Day, Year]: [Insert time]

There has been increased online chatter concerning a possible attack targeting the U.S. transportation sector in your region. A known terrorist organization has come forward claiming responsibility for the failed bombing and is identified as a source of the online chatter.

There is no specific location discussed, but information distributed to [insert your region]’s Joint Terrorism Task Force (JTTF) alerts local law enforcement that [insert your freight yard] is a probable target.

## Discussion Questions

1. How would your organization anticipate managing this updated information?
2. What other agencies / organizations / stakeholders would your organization need to communicate this threat? Who is responsible for that notification?
3. What notification capabilities (e.g., alerts, email, telecom, SMS text, special tools) do you use to share information and help protect your critical infrastructure assets internally and to sector stakeholders?
4. If your organization heard rumors of this threat before any official notification was disseminated, what would your organization do with that information?
5. What security details, such as private or local law enforcement, does your organization employ daily?
6. Does the organization participate in Suspicious Activity Reporting (SAR) efforts?
7. What plans exist to prevent or deter an attack at your facility?
	1. What threats are you most concerned with preventing?
	2. Who is responsible for activating your security plan?
	3. What additional mitigation procedures might you implement?
	4. Are multiple agencies outside of your organization involved in the response and recovery planning process?
	5. Do your agencies and organizations cross-train on various attack scenarios?
	6. What measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased vigilance, etc.)?
	7. What physical deterrents does your facility have (e.g., closed-circuit television [CCTV], intrusion detection system [IDS], access control measures)?
8. How does this more direct understanding of the threat change your security positioning?
9. Do security personnel and employees receive IED Security Awareness training?
10. How are security and personnel trained to respond to a potential threat like this?
	1. Have security personnel had the opportunity to interact with local law enforcement?
	2. Which organizations contribute to the security of your facility?
	3. Have your facility employees and / or contractors received security awareness training and instruction on how to identify and report an intrusion?
	4. What are the rules of engagement for your security personnel?
	5. What is the chain of command for on-site security personnel?
11. Do your organization’s standard operating procedures (SOPs) include incident response roles and responsibilities for staff?
12. What security recommendations, if any, does your organization expect from local, state, and federal law enforcement?

This page is intentionally left blank.

# Module Two: Incident Response

## Scenario

### [Insert Month, Day, Year]: [Insert time + 8 days]

It is a calm, clear day at the [insert freight yard], and operations are in full swing. A train transporting toxic inhalation hazard (TIH) commodities that include chlorine gas and anhydrous ammonia is scheduled to depart [insert freight yard] at 10:00 a.m.

At 10:02 a.m., as the train transporting the TIH commodities departs the yard, an explosion occurs on the track. The explosion sets fire to the locomotive and damages 100 feet of track, causing the train to derail. Facility staff who heard the explosion are scrambling to respond as local emergency response agencies are dispatched to the scene.

By 10:05 a.m., local 911 operators begin receiving calls from [insert town / city] residents saying that there has been an explosion near the [insert freight yard]. Residents state that they can see plumes of smoke.

## Discussion Questions

1. What are your organization’s response priorities to this incident?
2. Do your organization’s emergency response plans (e.g., site security plans, emergency occupancy plans, emergency action plans, or other appropriate plans) contain protocol to deter / prevent an IED (e.g., i.d. screening, canine teams, etc.)?
	1. What training programs exist for personnel, and who trains them?
	2. How are personnel trained to respond to an IED?
3. What assets are on-site to immediately respond to an incident?
	1. What resources are available that would help with response?
	2. Does your facility have a dedicated or ancillary hazardous materials team on-site that is trained and equipped?
4. What protocols exist for notifying authorities to the incident, and how are any first responders notified?
	1. If the cell network is overwhelmed, does that affect your warning procedures?
	2. Are there alternate alert methods?
	3. How would the freight yard notify law enforcement to the presence of TIH commodities?
5. Does your organization set up an ICS at this time?
	1. When would you expect unified command to begin coming together?
	2. Are key agencies and facility personnel familiar with ICS procedures?
	3. What are each organization’s priorities at this stage of the incident?
	4. Which agencies are involved in the response?
	5. Which agency would have the lead in the response?
	6. How would law enforcement respond to the reports of an IED?
	7. How would the response change given the information about the chemicals on board the train?
	8. Are there any additional agencies or resources needed to address an IED / potential chemical spill?
	9. Are there any law enforcement SOPs that would affect other entities (i.e., moving fire / emergency medical services (EMS) out of an IED blast radius after the explosive is discovered, or potentially taking over nearby businesses for command posts or sniper positions)?
6. What protocols exist for alerting employees to an incident?
	1. What notification methods (e.g., alerts, emails, telecommunications, text message, special tools) does your facility use to send alert information?
7. Who is responsible for communicating incident information to the public?
	1. Does your organization have a designated Public Information Officer (PIO)? If so:
	2. What protocols exist for alerting partner organizations to an incident?
	3. Who is responsible for sending out the alerts or warnings?
	4. Do protocols exist for addressing media inquiries?
	5. How do PIOs receive information from the incident?
	6. Do you have canned public information templates for use in different kinds of incidents?
	7. Do you send out any notifications to the public using social media? If so, at what point in the incident would you expect to start sending out the notifications?
	8. Have your PIOs previously collaborated with other supporting organizations’ PIOs during a crisis?
8. Who is in charge of notifying state or federal agencies to the incident, and at what point in the incident would this occur?
	1. What resources or actions would you expect from state or federal agencies?
	2. How does your organization coordinate response operations with local, state, and federal agencies?
9. What steps are needed to ensure the area is cleared of threats?
10. Would there be any accountability taken of employees and, if so, how is it accomplished?
11. What are your evacuation procedures for an incident of this type?
	1. Are there established plans for a mass evacuation of both the facility as well as the greater community, if necessary?
		1. Who is responsible for activating the evacuation procedures?
		2. What training has been done on these plans?
		3. Is there is a specified rally point for evacuees?
		4. Would weather impact this location?
		5. Are there secondary and tertiary rally points in case the primary point is a part of the incident or evacuees overwhelm it?
	2. What plans or procedures exist to work with individuals with access and functional needs?

## Scenario Update

### [Insert Month, Day, Year]: [Insert time + 10 minutes]

The first responders dispatched from the first alarm arrive and begin their operations. As they begin to combat the fire and treat the many individuals who were hurt in the blast, victims denote “painful fumes” in the air in addition to the smoke from the fire. Some residents and others in the area have arrived on the scene and are taking photos from a distance and approaching employees asking what is going on.

Social media has erupted with various images and accounts of the incident following the explosion. Additionally, residents of [insert town / city] are reporting agitating fumes in the air, resulting in sinus pain and breathing troubles.

## Discussion Questions

1. What are your organization’s information sharing responsibilities at this point in the incident?
2. How do reports of “painful fumes” at the scene and from the public impact your response procedures?
3. Is a joint information center (JIC) established? If so, as what point in the incident did this happen?
	1. Where would the JIC be located?
	2. Which agencies would be involved in the JIC?
	3. How would agencies coordinate social media messaging?
	4. Is there a location where reporters know to gather when there is an incident?
	5. How are messages coordinated across the different agencies and organizations before activating the JIC?
	6. What social media monitoring capabilities can your organization use to maintain awareness of information spreading that may not be accurate?
		1. Who is responsible for mitigating misinformation?
		2. What procedures exist to counter false information on social media?
4. What information or warnings are being released to the public?
	1. Who is responsible for the initial messaging?
	2. How would you coordinate with local emergency management officials?
	3. How quickly is information being released?
	4. What methods are used to distribute information?
	5. What should the content of the messaging be?
	6. Is targeted information sent to businesses or people in the surrounding area?
5. How does the ongoing HAZMAT incident impact public messaging and coordination?

Do generic, pre-scripted public messages exist that can be adapted to a particular incident?

1. How would the medical response be conducted?
	1. Does [insert your facility name] have any medical staff trained to respond to this kind of incident?
	2. Which organizations and agencies are involved in the medical response?
	3. Which organization or agency would have the lead in the medical response?
	4. At what point would first responders’ protocols allow medical personnel to enter the scene and begin triage and treatment of the injured?
		1. What challenges would the chemical waste pose?
		2. What actions, if any, would EMS personnel be able to take once an IED was identified?
		3. What are EMS agencies’ procedures regarding entry into a warm zone?
		4. Do your EMS agencies have protective gear and training for tactical entry?
2. Would this incident be considered a mass casualty incident (MCI)?
	1. What plans exist to respond to an MCI?
	2. At what point would the hospitals be informed of the incident?
		1. Who is responsible for contacting the hospitals?
3. How would arriving state and federal resources integrate into the command structure and at which locations (unified command, area command, emergency operations center [EOC], Multi-Agency Coordination [MAC] Group, etc.)?
4. Would there be sufficient resources immediately available to begin stabilizing the incident scene?
5. What mutual aid agreements, if any, does your organization have in place with other organizations?
	1. Are these mutual aid agreements formal or informal?
	2. Would the aid be automatic, or would you have to request it?
		1. If requested, whom would you contact, and how would you contact them?
		2. Do you have a backup contact and communication method in case you cannot use the primary?
	3. What are the financial considerations of the mutual aid agreements?
	4. Are there any limitations to what mutual aid can do (legal, procedural, equipment, etc.)?
	5. How do you manage personnel that self-deploy?
6. What role do city and county governments play in the ongoing response?
7. If this were declared a terrorist incident, what impact would that have on the response?
	1. How would that determination impact state and federal involvement?
	2. If it were determined a terrorist organization backed the attacker, as opposed to a lone wolf drawing inspiration from a terrorist organization, what impact would that have?
8. What is the process to collect evidence that belongs to citizens (cell phone videos, cameras, security footage from private businesses, etc.)?

# Module Three: Short-term Recovery

## Scenario

### [Insert Month, Day, Year]: [Insert Time + 45 minutes]

[Insert local hospital] indicates that their ER is burdened with the intake of residents adjacent to the incident describing eyes and nose irritation, coughing, blood in the sputum, and shortness of breath along with chest pain.

[Name of local freight yard] and the local community has turned to short-term recovery procedures. Residents are rushing to local stores to buy air purifiers. The freight yard is closed off for further investigation and all trains scheduled to run through the yard must be rerouted.

## Discussion Questions

1. How would resources be coordinated between the MCI and HAZMAT incident?

Who is responsible for that coordination?

What other city / county resources would be used, and how will that occur?

1. Would family assistance or reunification centers be set up following the incidents?
	1. If so, who is responsible for this?
	2. What procedures exist for this?
	3. How are families made aware of where to go?
	4. At what point in time would these centers be set up?
	5. Which agencies are involved, and who is responsible for leading this aspect of the recovery?
	6. Which facilities would be used?
	7. How are victims and family members made aware of the location?
	8. Which agency or person, if any, would be in charge of setting up these locations?
2. How do you determine the security of your freight rail yards and rail cars after an incident?
3. Based on the scenario, how would the damage impact operations?
4. Does your business have a continuity of operations plan?
	1. Does your continuity of operations plan include a crisis communications plan?
5. How and what type of messaging will be sent to employees and people in the surrounding community?
	1. Who makes the decision to send these messages?
	2. What training do employees receive regarding media relations and the release of sensitive information?
6. What are the priorities at your business post-incident?
	1. Do your plans, policies, or procedures specify these priorities?
	2. How is this communicated internally?
	3. Are priorities coordinated with county emergency management?
	4. Are priorities coordinated with state or federal agencies?
7. How are personal items reunited with their owners if left at the scene?
8. What would the financial impact be on your organization if it were closed because of such an incident?
	1. What are the implications of being unable to use the tracks or freight rail yard for a period of time?
9. Would your organization be responsible for responding to the impact this incident has had on your greater community?
10. What local, state, or federal resources are available to assist in recovery or business continuity?
	1. Does your organization have memorandums of understanding with local response agencies?
11. How is information communicated with personnel and families during the days following the incident?
12. Does your organization have mental health services available for your employees?
	1. What SOPs, if any, do you have in place for residents the incident impacted?
	2. How would available services be communicated?
13. What health care or insurance does your organization provide to cover potential medical costs for staff impacted by this chemical spill?
	1. Do you have a continuity plan that considers if staff members may be on disability during the organization’s short-term recovery?
14. What information are you communicating with the public?
	1. Who in your organization is responsible for this communication?
	2. How is your organization communicating and ensuring the safety of residents?
	3. Do your plans, polices, and procedures outline this?
15. How will your organization restore public confidence following this type of incident?
16. What is your plan to handle the significant media attention from national and international outlets?
17. At what point would you consider your organization back to steady state operations?
18. Following this attack, what additional protective measures will be put in place at your organization or in your community?
	1. How would information on protective measures be obtained?
	2. How would any relevant classified information be shared?
	3. How is relevant information shared within your critical infrastructure sector?
		1. How do you communicate information to other members of your sector or receive information from them?
		2. Do you know how to contact your Sector Specific Agency (SSA)?
		3. Do you have a Homeland Security Information Network (HSIN) account?
	4. Do you know how to contact your CISA Protective Security Advisor (PSA)?
	5. If you are a Chemical Facility Anti-Terrorism Standards (CFATS) covered facility, how do you contact your CISA Chemical Security Inspector (CSI)?
19. Who makes the decision on when the area will be reopened?
	1. How is that decision communicated to the public and the media?
20. Are there contracts in place to assist in the cleanup of the area prior to reopening?
21. Does your community or organization have a plan for the management of donations or public memorials?
22. What would you consider the “new normal” for your organization and community?
23. What recovery activities will continue after your community transitions from long-term recovery to the “new normal?”
24. Are there any long-term cascading impacts or interdependencies for your sector stemming from this incident?
	1. How would this information be shared with federal, state, and local agencies?

This page is intentionally left blank.

# Appendix A: Exercise Participants

| **Participating Private Sector Organizations** |
| --- |
| [Insert private sector participants] |
|  |
|  |
|  |

| **Participating Local Organizations** |
| --- |
| [Insert local participants] |
|  |
|  |
|  |

| **Participating State Organizations** |
| --- |
| [Insert state participants] |
|  |
|  |
|  |

| **Participating Federal Organizations** |
| --- |
| [Insert federal participants] |
|  |
|  |
|  |

| **Other Participating Organizations** |
| --- |
| [Insert other participants] |
|  |
|  |
|  |

This page is intentionally left blank.

# Appendix B: Relevant Plans

![NTAS Alerts: Sample NTAS alert. Sample reads as follows:   HEADER: National Terrorism Advisory System Alert  www.dhs.gov/advisories  [Insert Date]  DURATION: [Insert issued date and time] - [Insert date and time 4 months later]  TYPES OF ADVISORIES:   DETAILS:  - The Department of Homeland Security in consultation with the Federal Bureau of Investigation has reviewed nearly gathered intelligence and has deemed there to be a credible threat against the transportation systems sector. - Current intelligence indicates that an attack could be focused on train/freight stations, airports, ports, or bus stops, using improvised explosive devices in backpacks or duffle bags -Authorities are currently investigation a number of domestic terrorist groups within the United States with ties to international terrorist organizations - Local law enforcement authorities are encouraged to work with their private sector partners to ensure they are aware of the Elevated Threat status.  HOW YOU CAN HELP:  The public can assists authorities by reporting any suspicious activity they see. To report suspicious activity, the public should contract their local law enforcement agency and described specifically what was observed:  - Who or what you saw   - When you saw it  - Where it occurred; and   - Why its suspicious  BE PREPARED:  - The public should ensure they are aware of their surroundings when at major transportation sites   STAY INFORMED:  - DHS NTAS Website: http://www.dhs.gov/alerts and http://twitter.com/NTASAlerts http://dhs.gov/see-something-say-something  FOOTER: If you see something, say something. Report suspicious activity to local law enforcement or call 911  The National Terrorism Advisory System provides Americans with alert information on homeland security issues and threats. It is distributed by the Department of Homeland Security. More information is available at: www.dhs.gov/advisories. To receive mobile updates: www.twitter.com/dhsgov ]()

**Figure 1. National Terrorism Advisory System Alert Example**

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix C: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CCTV** | Closed-Circuit Television |
| **CFATS** | Chemical Facility Anti-Terrorism Standards |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CSI** | Chemical Security Inspector |
| **CTEP** | CISA Tabletop Exercise Package |
| **DHS** | Department of Homeland Security  |
| **EMS** | Emergency Medical Services |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **HAZMAT** | Hazardous Materials Management  |
| **HSIN** | Homeland Security Information Network |
| **ICS** | Incident Command System |
| **IDS** | Intrusion Detection System |
| **IED** | Improvised Explosive Device  |
| **IP** | Improvement Plan |
| **JIC** | Joint Information Center |
| **JTTF** | Joint Terrorism Task Force |
| **MAC** | Multi-Agency Coordination |
| **MCI** | Mass Casualty Incident  |
| **NIMS** | National Incident Management System |
| **NTAS** | National Terrorism Advisory System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SOP** | Standard Operating Procedures |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Experts |
| **SSA** | Sector Specific Agency |
| **TIH** | Toxic Inhalation Hazard |
| **TTX** | Tabletop Exercise  |

